MATH491

Summer Research Project

2006– 2007

Fibonacci Numbers and some Applications to Digital Image Scrambling

Benjamin Williams

Department of Mathematics and Statistics
University of Canterbury

Fibonacci Numbers and some Applications to Digital Image Scrambling

Ben Williams

February 9, 2007

Abstract

An analysis of some recently proposed methods of digital image scrambling that use Fibonacci numbers. This report describes the mathematics required to understand why these methods work.

Contents

1 Introduction

Digital image scrambling is a method to hide the content of an image. One application is in satellite television broadcasting systems to prevent unauthorized viewing. The scrambling algorithm needs to be fast so that each frame can be de-scrambled in real-time. A method used in the past has been to permute the rows of the image. A key is then required to describe the inverse permutation.

Other methods of scrambling include scrambling pixel positions or scrambling the color values of each pixel. Without knowledge of the key it should be difficult to recover the scrambled image given time constraints.

Digital image scrambling methods have specific requirements that general data encryption algorithms may not provide. The algorithms need to be simple and fast so that they can be used by low cost equipment. The scrambled image should not adversely affect data compression algorithms and information about the image such as dimension needs to be available without decrypting the image.

In order to understand the new scrambling methods proposed in [2], [3], [4], some properties of the Fibonacci numbers are described. Affine transformations are then presented because these will be used to scramble pixels to new positions within an image. Some affine transformations that use Fibonnacci numbers for scrambling digital images are described and analysed.

2 Properties of the Fibonacci numbers

Definition 2.1. The *Fibonacci numbers* are the numbers in the sequence 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ... , where the nth Fibonacci number f_n is defined by the linear recurrence relation

$$f_n = f_{n-1} + f_{n-2} \qquad \text{for } n \geq 2 \text{ and } f_0 = 0, f_1 = 1.$$

Theorem 2.1. *f_n is even $\iff$ 3 divides n.*

Proof. Consider the Fibonacci sequence where each number is reduced modulo 2.

$$\begin{aligned} s_n &= f_n \mod 2 \\ s_n &= f_{n-1} + f_{n-2} \mod 2 \\ s_n &= s_{n-1} + s_{n-2} \mod 2 \end{aligned}$$

The sequence generated is

$$0, 1, 1, 0, 1, 1, 0, 1, 1, 0 \ldots$$

The period of the sequence is 3 because $s_i = s_{i+3}$ for all $i \in \mathbb{N}$. It follows that

$$\begin{aligned} s_{3k} &= 0 \\ s_{3k+1} &= 1 \\ s_{3k+2} &= 1 \quad \text{for all } k \in \mathbb{N}. \end{aligned}$$

Therefore $f_n = 0 \mod 2 \iff n = 3k$. □

Definition 2.2. The *Fibonacci matrix* is the 2×2 matrix

$$F = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

It is used to represent the Fibonacci sequence as a matrix equation.
Let $\mathbf{u}_n = \begin{bmatrix} f_{n-1} \\ f_n \end{bmatrix}$. Then for $n \geq 1$, $\mathbf{u}_{n+1} = F\ \mathbf{u}_n$.

Theorem 2.2.

$$f_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$$

Table 1: The Fibonacci numbers

n	f_n	f_{n+1}	$f_n^2 \mod f_{n+1}$
0	0	1	0
1	1	1	0
2	1	2	-1
3	2	3	1
4	3	5	-1
5	5	8	1
6	8	13	-1
7	13	21	1
8	21	34	-1
9	34	55	1
10	55	89	-1
11	89	144	1
12	144	233	-1
13	233	377	1
14	377	610	-1
15	610	987	1
16	987	1597	-1

Proof. [5] p. 355.

$$\begin{aligned}
\mathbf{u}_{n+1} &= F\ \mathbf{u}_n \\
&= F\ (F\ \mathbf{u}_{n-1}) \\
&= F^2\ \mathbf{u}_{n-1} \\
&\vdots \\
&= F^n\ \mathbf{u}_{n-(n-1)} \\
&= F^n\ \mathbf{u}_1
\end{aligned}$$

λ is an eigenvalue of F if $\det(F - \lambda I) = 0$. Solving the characteristic equation for F gives eigenvalues

$$\lambda_1 = \frac{1+\sqrt{5}}{2}, \qquad \lambda_2 = \frac{1-\sqrt{5}}{2}$$

Let $\mathbf{v}_1$ and $\mathbf{v}_2$ be corresponding eigenvectors. These eigenvectors are linearly independent because $\lambda_1 \neq \lambda_2$, therefore they span $\mathbb{R}^2$.
Let $\mathbf{u}_1 = c_1\mathbf{v}_1 + c_2\mathbf{v}_2$.

$$\begin{aligned}
\mathbf{u}_{n+1} &= F^n\ \mathbf{u}_1 \\
&= F^n(c_1\mathbf{v}_1 + c_2\mathbf{v}_2) \\
&= c_1F^n\mathbf{v}_1 + c_2F^n\mathbf{v}_2) \\
\begin{bmatrix} f_n \\ f_{n+1} \end{bmatrix} &= c_1\lambda_1^n\mathbf{v}_1 + c_2\lambda_2^n\mathbf{v}_2
\end{aligned}$$

Therefore $f_n = d_1\lambda_1^n + d_2\lambda_2^n$ for coefficients yet to be determined. Solving system of equations

$$f_0 = d_1\lambda_1^0 + d_2\lambda_2^0 = d_1 + d_2 = 0$$

$$f_1 = d_1\lambda_1^1 + d_2\lambda_2^1 = d_1\left(\frac{1+\sqrt{5}}{2}\right) + d_2\left(\frac{1-\sqrt{5}}{2}\right) = 1$$

gives $d_1 = \frac{1}{\sqrt{5}}$, $d_2 = \frac{-1}{\sqrt{5}}$.

$$\begin{aligned}
f_n &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)\right)^n \\
&= \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}
\end{aligned}$$

□

Lemma 2.3. *For $n \geq 1$*

$$F^n = \begin{bmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{bmatrix}$$

Proof. By induction.
Let $P(n)$ be the proposition that $F^n = \begin{bmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{bmatrix}$.
$P(1)$ is the proposition that $F = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ which is true.
If $P(k)$ is true for some positive integer k then

$$\begin{aligned} F^k F &= \begin{bmatrix} f_{k-1} & f_k \\ f_k & f_{k+1} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \\ &= \begin{bmatrix} f_k & f_{k-1} + f_k \\ f_{k+1} & f_k + f_{k+1} \end{bmatrix} \\ &= \begin{bmatrix} f_k & f_{k+1} \\ f_{k+1} & f_{k+2} \end{bmatrix} \\ &= \begin{bmatrix} f_{(k+1)-1} & f_{k+1} \\ f_{k+1} & f_{(k+1)+1} \end{bmatrix} \\ &= F^{k+1} \end{aligned}$$

Therefore $P(k) \Rightarrow P(k+1)$ and by induction, $P(n)$ is true for all $n \geq 1$. □

Theorem 2.4. *Let f_n denote the nth Fibonacci number. Then for $n \geq 1$*

$$f_{n-1} \cdot f_{n+1} - {f_n}^2 = (-1)^n$$

Proof. [7]
Taking determinants on both sides of equation in Lemma 2.3 gives

$$\begin{vmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{vmatrix} = \det(F^n) = \det(F)^n = (-1)^n$$

□

Theorem 2.5. *Any two consecutive Fibonacci numbers f_n and f_{n+1} are relatively prime.*

Proof. By induction.
Let $P(n)$ be the proposition that $\gcd(f_n, f_{n+1}) = 1$.

$P(0)$ is the proposition that $\gcd(0,1) = 1$ which is true.
If $P(k)$ is true for some positive integer k then

$$\gcd(f_k, f_{k+1}) = 1 = \gcd(f_k + f_{k+1}, f_{k+1}) = \gcd(f_{k+1}, f_{k+2})$$

because $f_k + f_{k+1} = f_{k+2}$ by Definition 2.1.

Therefore $P(k) \Rightarrow P(k+1)$ and by induction, $P(n)$ is true for all $n \geq 0$. □

3 Affine transformations

Let $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. Denote $\mathbb{Z}_m^n$ as the set of vectors of dimension n with each component an element in $\mathbb{Z}_m$. Denote $M_n(\mathbb{Z}_m)$ as the set of all $n \times n$ matrices with each entry an element in $\mathbb{Z}_m$. Matrix operations addition and multiplication over $\mathbb{Z}_m$ are defined the same as addition and multiplication over $\mathbb{Z}$ with each matrix entry reduced modulo m.

For example: Let $A = (a_{i,j})$, $B = (b_{i,j}) \in M_n(\mathbb{Z}_m)$ and $m \in \mathbb{N}$.
We write

$$A = B \mod m$$

if $a_{i,j} = b_{i,j} \mod m$ for all $i, j \in \{0, 1, \ldots, n\}$.

Definition 3.1. If there exists $A' \in M_n(\mathbb{Z}_m)$ such that $AA' = I_n \mod m$ then A is *invertible* $\mod m$.

Theorem 3.1. *Let $A \in M_n(\mathbb{Z}_m)$ and $m \in \mathbb{N}$.*
A is invertible $\iff$ $\det(A)$ and m are relatively prime.

Proof. [4] p. 94.
Suppose A is invertible. Then $AB = I \mod m$ for some $B \in M_n(\mathbb{Z}_m)$.

$$\begin{aligned} \det(AB) &= 1 \mod m \\ \det(A) \cdot \det(B) &= 1 \mod m \end{aligned}$$

Let $a = \det(A)$ and $b = \det(B)$.

$$ab + km = 1 \text{ for some } k \in \mathbb{Z}$$

Suppose $c|a$ and $c|m$. Then $c|(ab + km)$ i.e. $c|1$. Therefore $\gcd(a, m) = 1$.

Conversely suppose $\gcd(a, m) = 1$. Then

$$\begin{aligned} ab + km &= 1 \text{ for some } b, k \in \mathbb{Z} \\ ab &= 1 \mod m \end{aligned}$$

A well known equation for square matrices is

$$A \text{ adj}(A) = \det(A)\ I$$

where adj(A) is the *adjoint* matrix of A. This equation gives a formula to calculate A^{-1}.

$$\begin{aligned} A \text{ adj}(A) &= \det(A)\ I \mod m \\ bA \text{ adj}(A) &= ba\ I \mod m \\ A\ b \text{ adj}(A) &= I \mod m \\ A^{-1} &= b \text{ adj}(A) \mod m \end{aligned}$$

□

Remark 1. If $det(A) = 0$ then A is not invertible, since $\gcd(0, m) = m$. An example of a non-invertible matrix with a non-zero determinant is $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ $over M_2(\mathbb{Z}_4)$.

Definition 3.2. A transformation $T : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ defined by $T(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$ mod m for some $\mathbf{b} \in \mathbb{Z}_m^n$, $A \in M_n(\mathbb{Z}_m)$ is called *affine*. If $\mathbf{b} = 0$, then T is a *linear* transformation.

Corollary 3.2. *The affine linear map from Definition 3.2 is bijective if and only* det(A) *and* m *are relatively prime.*

Definition 3.3. Let $A \in M_n(\mathbb{Z}_m)$ and $m \in \mathbb{N}$.

A is *periodic* if there exists $t \in \mathbb{N}$ such that $t > 0$ and $A^t = I_n$. The *period* of A is the smallest positive integer t such that $A^t = I_n$.

An affine transformation $T : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ is *periodic* if $T^t(\mathbf{x}) = \mathbf{x}$ for some positive integer t and all $\mathbf{x} \in \mathbb{Z}_m^n$.

Theorem 3.3. *Let* $A \in M_n(\mathbb{Z}_m)$ *and* $m \in \mathbb{N}$.
A *is periodic* $\iff$ A *is invertible.*

Proof. Suppose A is periodic. Then for some postive integer t

$$\begin{aligned} A^t &= I \mod m \\ A\ A^{t-1} &= I \mod m \end{aligned}$$

Therefore A is invertible.

Conversely, suppose A is invertible. There are exactly m^{n^2} distinct matrices in $M_n(\mathbb{Z}_m)$.

Define the multiset $S = \{A^i \mod m : 0 \leq i \leq m^{n^2}\}$.
There exists $A^k, A^l \in S$ where $k \leq l$ and $A^k = A^l$.

$$\begin{aligned} A^k &= A^l \mod m \\ A^k\,(A^{-1})^k &= A^l\,(A^{-1})^k \mod m \\ I &= A^{l-k} \mod m \end{aligned}$$

Therefore A is periodic. □

Theorem 3.4. *The affine transformation $T : \mathbf{x} \to A\mathbf{x} + c\mathbf{b}$ defined in 3.2 is periodic if and only if A is invertible.*

Proof. Define affine transformation $S : \mathbb{Z}_m^{n+1} \to \mathbb{Z}_m^{n+1}$ by

$$S(\mathbf{v}) = \begin{bmatrix} A & \mathbf{b} \\ \mathbf{0}^T & 1 \end{bmatrix} = A'\mathbf{v}$$

Let $\mathbf{y} = \begin{bmatrix} \mathbf{x} \\ c \end{bmatrix}$ for some $c \in \mathbb{Z}_m, \mathbf{x} \in \mathbb{Z}_m^n$. Then

$$S(\mathbf{y}) = \begin{bmatrix} A & \mathbf{b} \\ \mathbf{0}^T & 1 \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ c \end{bmatrix} = \begin{bmatrix} A\mathbf{x} + c\mathbf{b} \\ c \end{bmatrix} = \begin{bmatrix} T(\mathbf{x}) \\ c \end{bmatrix}$$

Let $P(n)$ be the proposition that

$$S^n(\begin{bmatrix} \mathbf{x} \\ c \end{bmatrix}) = \begin{bmatrix} T^n(\mathbf{x}) \\ c \end{bmatrix}$$

$P(1)$ has been proved.

If $P(k)$ is true, then

$$S^{k+1}(\mathbf{y}) = S(S^k(\mathbf{y})) = \begin{bmatrix} A & \mathbf{b} \\ \mathbf{0}^T & 1 \end{bmatrix} \begin{bmatrix} T^k(\mathbf{x}) \\ c \end{bmatrix} = \begin{bmatrix} A\,T^k(\mathbf{x}) + c\mathbf{b} \\ c \end{bmatrix} = \begin{bmatrix} T^{k+1}(\mathbf{x}) \\ c \end{bmatrix}$$

Therefore $P(k) \Rightarrow P(k+1)$ and by induction, $P(n)$ is true for all $n \geq 1$.

If there exists positive integer t such that

$$S^t(\begin{bmatrix} \mathbf{x} \\ c \end{bmatrix}) = \begin{bmatrix} T^t(\mathbf{x}) \\ c \end{bmatrix} = \begin{bmatrix} \mathbf{x} \\ c \end{bmatrix}$$

then S and T are both periodic, otherwise S and T are both non-periodic.

T is periodic $\iff$ S is periodic
T is periodic $\iff$ A' is invertible (Theorem 3.3)
T is periodic $\iff$ there exists $A'^{-1} = \begin{bmatrix} A^{-1} & A^{-1}(-\mathbf{b}) \\ \mathbf{0}^T & 1 \end{bmatrix}$
T is periodic $\iff$ A is invertible

□

Remark 2. Any scalar multiple of $\mathbf{b}$ can be used in T and the period will remain the same.

4 Applications to digital image scrambling

Definition 4.1. The *Fibonacci affine transformation* $T : \mathbb{Z}_m^2 \to \mathbb{Z}_m^2$ is defined by $T(\mathbf{x}) = F\mathbf{x} + \mathbf{b} \mod m$ for some $\mathbf{b} \in \mathbb{Z}_m^2$, $m \in \mathbb{N}$ and F from Definition 2.2.

Proposition 4.1. *The Fibonacci affine transformation is periodic.*

Proof. $\gcd(\det(F), m) = 1$ for all m, so by Theorems 3.1 and 3.4, the transformation is periodic. □

The Fibonacci matrix transformation is described in [3] where the authors use it to scramble images of dimension $m \times m$ pixels. Each pixel has a coordinate in $\mathbb{Z}_m^2$ that can be scrambled to a new coordinate by T. The period of the transformation varies for different m. The suggested scrambling method is to apply T on every pixel of the image. Then to decrypt, repeatedly apply T to the scrambled image until the original image is recovered. It is unclear why the inverse transformation of T is not used to make the decryption quicker. The vector $\mathbf{b}$ can be used as a key. Different values of $\mathbf{b}$ will affect the period of T.

Definition 4.2. The *Arnold transformation* $T : \mathbb{Z}_m^2 \to \mathbb{Z}_m^2$ is defined by $T(\mathbf{x}) = A\mathbf{x} \mod m$ for $m \in \mathbb{N}$ and

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

The Arnold transformation works the same way as the Fibonacci matrix transformation. The Arnold transformation is also periodic for all m.

Remark 3. $F^2 = A$

Another transformation described in [4] works as follows.

Definition 4.3. $T : \mathbb{Z}_m^2 \to \mathbb{Z}_m^2$ defined by $T(\mathbf{x}) = B\mathbf{x} + \mathbf{b} \mod f_{n+1}$ for some $\mathbf{b} \in \mathbb{Z}_m^2$, $m \in \mathbb{N}$ with

$$B = \begin{bmatrix} f_n & 0 \\ 0 & f_n \end{bmatrix}$$

Proposition 4.2. *B is invertible, hence the transformation is periodic.*

Proof. $\det(B) = f_n^2 = f_{n-1}f_{n+1} + (-1)^{n+1}$ by Theorem 2.4.
If $c \mid \det(B)$ and $c \mid f_{n+1}$ then $c \mid 1$, therefore $\det(B)$ and f_{n+1} are coprime. □

Proposition 4.3. *When n is odd the period of B is 2. When n is even the period of B is 4.*

Proof. From Theorem 2.4 we have

$$f_n{}^2 = (-1)^{n+1} \mod f_{n+1}$$

so $f_n{}^4 = 1 \mod f_{n+1}$ and $B^4 = I \mod f_{n+1}$.

If B has period t then $t|4$.
When n is even $B \neq I$ and $B^2 = -I \mod f_{n+1}$. Therefore when n is even the period of B is 4.

When n is odd, $f_n{}^2 = 1 \mod f_{n+1}$, so $B^2 = I \mod f_{n+1}$. Since $B \neq I \mod f_{n+1}$, when n is odd the period of B is 2. □

Remark 4. Although B has period 2 or 4, the period of the *transformation* may not be 2 or 4 when $\mathbf{b}$ is non-zero.

The transformation permutes the columns and rows of the image by the permutation $R : k \to kf_n + b \mod f_{n+1}$ where k is a column or row number in $\{1, 2, \ldots, f_{n+1} - 1\}$. The authors in [4] also include zero in this set but zero is a fixed point when $b = 0$. The authors state that having a period of 2 or 4 is efficient because encryption and decryption are the same functions and decryption can be achieved by reapplying the transformation.

The case where $b = 0$ will be examined. Let $S : k \to kf_n \mod f_{n+1}$ for k in $\{1, 2, \ldots, f_{n+1} - 1\}$. It follows from Proposition 4.3 that S has period 4 if n is even and period 2 if n is odd.

Definition 4.4. A *uniform permutation* is a permutation in which all disjoint cycles are of the same length. This means there are no fixed points unless the permutation is the identity.

Remark 5. If a permutation has period t, then the length of each cycle divides t, since t is the lowest common multiple of all cycle lengths.

Suppose the columns or rows of an image are scrambled using a uniform permutation. Then every row or column is moved, so the image content may be hidden more effectively than a permutation that leaves some rows or columns unchanged.

In general the permutation S is not uniform. Fixed points can be found by solving x in the equation

$$xf_n = x \mod f_{n+1}. \tag{1}$$

Proposition 4.4. *For $n > 3$,*
If n is odd then S is not uniform.

Proof. $x = k(f_n + 1) \quad k \in \mathbb{N}$ gives solutions to equation (1) .

$$\begin{aligned} k(f_n + 1) \cdot f_n &= k(f_n^2 + f_n) \mod f_{n+1} \\ &= k(1 + f_n) \mod f_{n+1} \end{aligned}$$

Remark 6. When $n = 3$, S is uniform.

□

Proposition 4.5. *If n is even, then S has no transpositions.*

Proof. A transposition exists if

$$x = f_n^2 x \mod f_{n+1} \tag{2}$$

and

$$x \neq f_n x \mod f_{n+1} \tag{3}$$

for some $x \in \{1, 2, \ldots, f_{n+1} - 1\}$. This proof will show that if equation (2) has a solution, then $x = f_n x \mod f_{n+1}$ has the same solution.

Solutions are found by solving for x:

$$\begin{aligned} x &= f_n^2 x \mod f_{n+1} && (4) \\ x &= -x \mod f_{n+1} && (5) \\ 2x &= 0 \mod f_{n+1} && (6) \end{aligned}$$

A solution exists $\iff$ 2 divides f_{n+1}, then $x = \frac{f_{n+1}}{2}$.

f_{n+1} is even, so by Theorem 2.1, f_n is odd.

$$\begin{aligned} f_n x &= (2m + 1)x \mod f_{n+1} \\ &= (2m)\frac{f_{n+1}}{2} + \frac{f_{n+1}}{2} \mod f_{n+1} \\ &= m f_{n+1} + x \mod f_{n+1} \\ f_n x &= x \mod f_{n+1} \end{aligned}$$

This is a contradiction to equation (3). Therefore, no transpositions exist. □

Proposition 4.6. *For even n,*
S is uniform $\iff$ f_{n+1} is odd.

Proof. Suppose S is uniform, then no fixed points exist.
If $x = f_n x \mod f_{n+1}$ has no solutions then by Proposition 4.5

$$x = f_n^2 x \mod f_{n+1} \tag{7}$$
$$2x = 0 \mod f_{n+1} \tag{8}$$

has no solutions so f_{n+1} is odd.

Conversely, suppose f_{n+1} is odd and a fixed point x exists. Then equation (8) has no solution thus

$$x = f_n^2 x \mod f_{n+1}$$

has no solution. But a fixed point exists so

$$x = f_n x = f_n^2 x \mod f_{n+1}$$

This is a contradiction. □

Proposition 4.7. *For even n,*
f_{n+1} is odd $\iff$ n equals 0 or 4 mod 6.

Proof. Let f_{n+1} be odd, then by Theorem 2.1 either

$$n + 1 = 3k + 1 \implies n = 3k$$

or

$$n + 1 = 3l + 2 \implies n = 3l + 1$$

Equivalently, f_{n+1} is odd $\iff$ $n = 3k$ or $n = 3l + 1$. Now restrict n to even values so let $k = 2m$ and $l = 2m + 1$. Then

$$n = 6m$$

or

$$n = 3(2m + 1) + 1$$
$$n = 6m + 4$$

Therefore, for even n, f_{n+1} is odd $\iff$ $n = 6m$ or $n = 6m + 4$. □

5 Conclusion

The Fibonacci transformation and the Arnold transformation can be used on square images of any size. The period of the transformation will vary for different size images. The period of $F \mod m$ can be as large as $6m$ so the decryption process described could be very inefficient.

The transformation in definition 4.3 transforms pixels of an $f_{n+1} \times f_{n+1}$. In most practical cases, images are unlikely to be square and of this dimension. In this case the image can be cropped to $f_{n+1} \times f_{n+1}$ so that the transformation can be applied. Alternatively, a large Fibonacci number can be choosen that exceeds the dimensions of the image. But this would generate an encrypted image larger than the unencrypted image. Due to these limitations, the transformations do not appear to be very practical.

APPENDIX

Methods to calculate f_n in $\mathbb{Z}_m$

To calculate the nth Fibonacci number mod m, the equation in theorem 2.2 can be used and then f_n can be reduced modulo m. For very large n, this is infeasible. If F can be diagonalized over $\mathbb{Z}_m$ then calculating F^n is fast.

Eigenvalues of F exist if for non-zero vector $\mathbf{x}$,

$$\begin{aligned} F\,\mathbf{x} &= \lambda\mathbf{x} \mod m \\ F\,\mathbf{x} - \lambda\mathbf{x} &= \mathbf{0} \mod m \\ (F - \lambda I)\mathbf{x} &= \mathbf{0} \mod m \end{aligned}$$

Therefore λ is an eigenvalue of F if

$$\gcd(\det(F - \lambda I), m) > 1$$

The characteristic polynomial of F is $p(\lambda) = \det(F - \lambda I) = \lambda^2 - \lambda - 1$.
For example: $\lambda_1 = 3$ and $\lambda_2 = 8$ are eigenvalues of F in $\mathbf{Z}_{10}$ because $p(3) = 5$ and $p(8) = 5$ and $\gcd(5, 10)1$.

$$E_3 = \text{null}\begin{bmatrix} -3 & 1 \\ 1 & -2 \end{bmatrix} = \text{null}\begin{bmatrix} 7 & 1 \\ 1 & 8 \end{bmatrix} = \text{null}\begin{bmatrix} 1 & 8 \\ 7 & 1 \end{bmatrix} = \text{null}\begin{bmatrix} 1 & 8 \\ 0 & 5 \end{bmatrix} = \text{span}\begin{bmatrix} 6 \\ -2 \end{bmatrix}$$

$$E_8 = \text{null}\begin{bmatrix} -8 & 1 \\ 1 & -7 \end{bmatrix} = \text{null}\begin{bmatrix} 2 & 1 \\ 1 & 3 \end{bmatrix} = \text{null}\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} = \text{null}\begin{bmatrix} 1 & 3 \\ 0 & 5 \end{bmatrix} = \text{span}\begin{bmatrix} 6 \\ -2 \end{bmatrix}$$

Although λ_1 and λ_2 are distinct, they have the same eigenspace so we do not have two linearly independent eigenvectors to diagonalize F.

Proposition .1. *If $m \mid p(\lambda_1)$ and $m \mid p(\lambda_2)$ for distinct eigenvectors λ_1 and λ_2, and $\gcd(\lambda_1 - \lambda_2, m) = 1$, then*

$$f_n = (\lambda_1 - \lambda_2)^{-1}(\lambda_1^n - \lambda_2^n) \mod m$$

Proof. If $m \mid p(\lambda)$ then $\lambda(\lambda - 1) = 1 \mod m$ and $\lambda(1 - \lambda_2) = -1 \mod m$.

$$E_\lambda = \text{null}\begin{bmatrix} -\lambda & 1 \\ 1 & 1 - \lambda \end{bmatrix} = \text{null}\begin{bmatrix} 1 & 1 - \lambda \\ -\lambda & 1 \end{bmatrix} = \text{null}\begin{bmatrix} 1 & 1 - \lambda \\ 0 & \lambda(1 - \lambda) + 1 \end{bmatrix}$$

$$= \text{null} \begin{bmatrix} 1 & 1-\lambda \\ 0 & 0 \end{bmatrix} = \text{span} \begin{bmatrix} \lambda - 1 \\ 1 \end{bmatrix}$$

Let $\mathbf{v}_1$ and $\mathbf{v}_2$ be eigenvectors corresponding to λ_1 and λ_2 and let $P = \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 \end{bmatrix}$.

$$\begin{aligned}
F &= PDP^{-1} \\
F^n &= PD^nP^{-1} \\
&= \begin{bmatrix} \lambda_1 - 1 & \lambda_2 - 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{bmatrix} \frac{1}{\det(P)} \begin{bmatrix} 1 & 1-\lambda_2 \\ -1 & \lambda_1 - 1 \end{bmatrix} \\
&= \frac{1}{\det(P)} \begin{bmatrix} \lambda_1 - 1 & \lambda_2 - 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \lambda_1^n & (1-\lambda_2)\lambda_1^n \\ -\lambda_2^n & (\lambda_1 - 1)\lambda_2^n \end{bmatrix} \\
&= \frac{1}{\det(P)} \begin{bmatrix} (\lambda_1 - 1)\lambda_1^n + (1-\lambda_2)\lambda_2^n & (\lambda_1 - 1)(1-\lambda_2)\lambda_1^n + (\lambda_1 - 1)(\lambda_2 - 1)\lambda_2^n \\ \lambda_1^n - \lambda_2^n & (1-\lambda_2)\lambda_1^n + (\lambda_1 - 1)\lambda_2^n \end{bmatrix} \\
F^n &= \begin{bmatrix} f_{n-1} & f_n \\ f_n & f_{n+1} \end{bmatrix} \\
f_n &= \frac{1}{\det(P)} \lambda_1^n - \lambda_2^n \mod m \\
f_n &= (\lambda_1 - \lambda_2)^{-1} (\lambda_1^n - \lambda_2^n) \mod m
\end{aligned}$$

□

Remark 7. If $m \mid p(\lambda_1)$ and $m \mid p(\lambda_2)$, this does not imply $\gcd(\lambda_1 - \lambda_2, m) = 1$. e.g. in $\mathbf{Z}_{55}$, $p(48) = 0 \mod 55$ and $p(8) = 0 \mod 55$ but $\gcd(48 - 8, 55) = 5$.

The eigenvalues in these examples have been found by trying each element in $\mathbb{Z}_m$. Eigenvalues can be found directly if the equation from Theorem 2.2 is used. There are some advantages to using prime m. When m is prime, 2 is invertible and a method to calculate $\sqrt{5}$ is possible for some primes. Also $\gcd(\lambda_1 - \lambda_2, m) = 1$ is always true, so the equation from Proposition .1 can be used once the eigenvalues have been found.

Definition .1. Given integers a and p,
if $x^2 = a \mod p$ for some $x \in \{1, 2, \ldots, p-1\}$ then a is a quadratic residue mod p.

Definition .2. Given odd prime p and integer a, the Legendre symbol is

$$(a/p) = a^{\frac{(p-1)}{2}} \mod p$$

Theorem .2. *For p an odd prime and $a \in \mathbf{Z}_p^*$*

$$a \text{ is a quadratic residue } \mod p \iff (a/p) = 1 \mod p$$

Proof. [9]
Suppose $x^2 = a \mod p$ for some $x \in \mathbf{Z}_p^*$. Then by using Fermat's Theorem

$$a^{\frac{(p-1)}{2}} = (x^2)^{\frac{(p-1)}{2}} = x^{p-1} = 1 \mod p$$

Suppose $(a/p) = 1$ and let $a = g^k$ for primitive $g \in \mathbf{Z}_p^*$ and $k \in \{1, 2, \ldots, p-1\}$. Note: this is always possible for prime p.

$$a^{\frac{(p-1)}{2}} = (g^k)^{\frac{(p-1)}{2}} = g^{k(\frac{p-1}{2})} = 1 \mod p \quad \text{(by assumption)}$$

$$g^{k(\frac{p-1}{2})} = g^{p-1} \mod p \quad \text{(because primitive)}$$

Therefore $(p-1) \mid k(\frac{p-1}{2})$, so k is even.
Then $a = g^k = g^{2m} = (g^m)^2$ for some $m \in \mathbf{N}$. Thus a is a quadratic residue. □

Theorem .3. Law of Quadratic reciprocity. *For distinct odd primes p and q,*

1. *If both p and q equal 3 mod 4, then either $(q/p) = 1$ or $(p/q) = 1$ but not both.*
2. *If p or q equal 1 mod 4, then $(q/p) = 1 \iff (p/q) = 1$.*

Proposition .4. *For odd prime p,*
5 is a quadradic residue $\iff$ p equals 1 or -1 mod 10.

Proof. By Quadratic reciprocity,

$$\begin{aligned}
(5/p) = 1 &\iff (p/5) = 1 \\
(5/p) = 1 &\iff p^{\frac{5-1}{2}} = 1 \mod 5 \\
(5/p) = 1 &\iff p^2 = 1 \mod 5 \\
(5/p) = 1 &\iff p = 1 \text{ or } p = -1 \mod 5 \\
(5/p) = 1 &\iff p = 5k \pm 1 \\
(5/p) = 1 &\iff p = 5(2m) \pm 1 \quad \text{(odd k gives even p).} \\
(5/p) = 1 &\iff p = 1 \text{ or } p = -1 \mod 10
\end{aligned}$$

□

Now that we can identify which primes have 5 a quadratic residue, there still remains the problem of calculating $\sqrt{5}$. In general, calculating square roots of quadratic residues has the same level of complexity as integer factorization [12].

Proposition .5. *For given integer a, if $p = 3 \mod 4$ then $\sqrt{a} = a^{\frac{(p+1)}{4}} \mod p$.*

Proof. Assume a is a quadratic residue. Then

$$\begin{aligned}
a^{\frac{(p-1)}{2}} &= 1 \mod p \\
aa^{\frac{(p-1)}{2}} &= a \mod p \\
a^{\frac{(p-1)}{2}+1} &= a \mod p \\
a^{\frac{(p+1)}{2}} &= a \mod p \\
\sqrt{a^{\frac{(p+1)}{2}}} &= \sqrt{a} \mod p \\
a^{\frac{(p+1)}{4}} &= \sqrt{a} \mod p
\end{aligned}$$

There is always a solution because $4 \mid (p+1)$. □

Remark 8. In the first 1000 primes the proportion that are of the form $10k \pm 1$ is 0.491. The proportion that are of the form $4k+3$ is 0.504. The proportion that satisfy both forms is 0.251.

References

[1] Buchmann J.A. *Introduction to Cryptography*, Springer-Verlag New York Inc, 2001.

[2] J. Zou, R. K. Ward, D. Qi *A new image scrambling method based on fibonacci numbers*, Proceedings of the 2004 International Symposium on Circuits and Systems ISCAS 2004, May 23-26, 2004, Vancouver, Canada, Vol 3. pg 965.

[3] J. Zou, X Tie, R. K. Ward, D. Qi *Some Novel Image Scrambling Methods Based on Affine Modular Matrix Transformation* , Journal of Information & Computational Science 2: 1 (2005) 223-227.

[4] J. Zou, R. K. Ward, D. Qi *The Generalized Fibonacci transformations and application to image scrambling*, Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on, Vol 3. pg 385.

[5] Poole, D. *Linear algebra : a modern introduction, 2nd Ed*, Australia : Belmont, CA : Thomson Brooks/Cole, 2006.

[6] W. Zeng, H. Yu, and C. Lin. *Multimedia security technologies for digital rights management* , Amsterdam ; Boston : Academic Press, 2006.

[7] http://en.wikipedia.org/wiki/Fibonacci_number

[8] http://mcraeclan.com/MathHelp/BasicNumberSquareQuadraticResidues.htm Read 30/11/2006.

[9] http://rooster.stanford.edu/~ben/maths/numbertheory/qr.html Read 30/11/2006.

[10] http://mathworld.wolfram.com/QuadraticResidue.html Read 30/11/2006.

[11] http://en.wikipedia.org/wiki/Quadratic_reciprocity Read 5/12/2006.

[12] http://en.wikipedia.org/wiki/Quadratic_residue Read 5/12/2006.